Anwenderbericht

In der IT-Sicherheit zählen nur 100 Prozent

ATEGRIS will nach ESAMIT-AUDIT Schritt für Schritt besser werden

IT-Sicherheit gewinnt für Gesundheitseinrichtungen zunehmend an Bedeutung. Sie läuft jedoch Gefahr in den Hintergrund zu rücken, da es nicht unmittelbar zur Wertschöpfung beiträgt. Anders in der ATEGRIS Holding mit seinen aktuell 13 Gesellschaften, darunter das Evangelische Krankenhaus Oberhausen und das Evangelische Krankenhaus Mühlheim. „Wir haben uns bewusst mit der Sicherheitslage auseinandergesetzt und wollten die Qualität der Informationssicherheit durch einen strukturierten Prozess weiter steigern – und das auch nach außen transparent darstellen“, fasst Dr. Martin Kuhrau, Fachbereichsleiter IT bei der ATEGRIS GmbH, die Situation zusammen. „Uns wurde klar, dass die Bedeutung von IT und Infrastruktur für die gesamte Organisation immer mehr zunimmt.“ Deshalb wollte sich die Fachabteilung mit 17 Mitarbeitern selber überprüfen und sicherstellen, dass sie alle geforderten Services in der geforderten Qualität erbringen kann.

Wie das aber gewährleisten? Den Schlüssel sah Dr. Kuhrau im ESAMIT-Audit von CETUS Consulting, einer neuartigen Prozessarchitektur für den medizinischen IT-Betrieb. Das Ergebnis sollte dann die Basis für einen IT-Strategieplan 2020 bilden. „Dort wollten wir definieren, wo wir stehen, wo wir hinwollen und wie wir unsere Ziele erreichen“, sagt der Fachbereichsleiter. Überzeugt hat CETUS die Verantwortlichen der ATEGRIS durch seine pragmatische und fundierte Herangehensweise. „Uns war wichtig, dass der externe Dienstleister unsere Branche mit all den speziellen Anforderungen und Einschränkungen kennt und weiß, wie ein Krankenhaus funktioniert“, definiert Tobias Puhe, Betriebsmanager und unter anderem für die Server- und Speicherinfrastruktur verantwortlich, die Auswahlkriterien. Dazu sei das ESAMIT-Modell breit gefächert, es berücksichtige Vorgaben von BSI, ISO und KRITIS genauso wie den IT-Grundschutz.

Ehrlichen Status quo erhoben

In das ESAMIT-Audit, das im Frühjahr 2016 startete, wurden alle Einrichtungen von ATEGRIS einbezogen. „Wir haben bewusst keine Vorbereitungen getroffen, da wir eine ehrliche und offene Bestandsaufnahme der Ist-Situation erreichen wollten“, sagt Dr. Kuhrau. Das Ziel war ein Reifegrad von 3 bis 4. Mit 49 Prozent ist die ATEGRIS GmbH schließlich im oberen Mittelfeld vergleichbarer Einrichtungen gelandet. „Viele, die sich dem Audit stellen, landen gerade bei 20 und 30 Prozent“, weiß Puhe. Im Rahmen des IT-Strategieplans 2020 will das Unternehmen mithilfe eines konkreten Maßnahmenkataloges und Projektplanes in den einzelnen Segmenten besser werden, den Reifegrad entsprechend erhöhen und am Ende das Ziel von 100 Prozent erreichen.

Erst einmal haben Dr. Kuhrau und seine Kollegen einen Einblick in die relativen Stärken und Schwächen zur IT-Sicherheit bekommen. Dabei sind Mankos zutage getreten, an denen er mit seinem Team arbeiten wird: „So liegen viele Verfahrensweisen als Konzept vor, sie werden größtenteils auch gelebt, allerdings sind sie nicht ausreichend dokumentiert und mit Verfahrensanleitungen hinterlegt“, weiß der IT-Leiter. Als Aufgabe hat er sich gestellt, die Konzepte konkret darzustellen und gegebenenfalls zu schärfen und sie dann deutlich an alle Mitarbeiter zu kommunizieren.

Es gibt aber auch Bereiche, denen das Audit einen guten Stand bescheinigt. Dazu gehören die Sicherheit des Personals, der Schutz vor physikalischen Zugängen und Umwelteinflüssen sowie das Management von Informationssicherheitsvorfällen. Luft nach oben gibt es noch in punkto Sicherheitsleitlinie oder zu Fragen der Kryptographie. „Hier

müssen wir uns allerdings die Frage stellen, ob wir die wollen und falls ja, wie wir sie umsetzen“, gibt Puhe zu bedenken.

Risiken erkennen und managen

Alles was die ATEGRIS tut, ist strukturiert und folgt einem Plan, der zusammen mit CETUS ausgearbeitet worden ist. Das Consulting-Unternehmen begleitet die Holding auch auf dem Weg, besonders intensiv im Jahr 2017. „Da gab es viele To-dos“, sagt Dr. Kuhrau. „Es gab viele Treffen bei uns, während derer wir alle Themen durchgearbeitet, Reviews gesichtet, eine Leitlinie entworfen sowie eine Struktur für die Risikobewertung aufgebaut haben.“ Im Zentrum der Betrachtung stand die Etablierung eines Information Security Management Systems, kurz ISMS. Das setzt die ATEGRIS auf einer im Hause bestehenden Plattform auf, die zu diesem Zweck erweitert wird. Bis Ende 2018 soll das System dann mit Inhalten und Leben gefüllt sein.

Beim Risikomanagement geht es darum, Risiken zu erkennen, sie zu bewerten und dann im Zweifelsfall entsprechende Maßnahmen abzuleiten. „Dazu haben wir gemeinsam mit CETUS eine Informationssicherheitsleitlinie erarbeitet und die intern verabschiedet“, so Dr. Kuhrau. Das zog auch strukturelle Veränderungen nach sich, beispielsweise wurde ein Board ins Leben gerufen, das regelmäßig zu dem Thema tagt. Ein weiterer Baustein ist Tobias Puhe. Er hat sich 2016 beim TÜV zum Informationssicherheitsbeauftragten, neudeutsch Information Security Officer, weitergebildet. Um den organisatorischen Hintergrund besser abdecken und interne Kontrollen noch effektiver strukturieren zu können, folgt in diesem Jahr die Fortbildung zum Chief Information Security Officer, dem CISO.

Redundanzen in der Prozesskette schaffen

Momentan steht der Aufbau des ISMS ganz oben auf der Agenda. Die wesentliche Herausforderung besteht darin, die komplexe Struktur der Systeme in der Beziehung untereinander abzubilden. „Dazu müssen wir eine gesamte Kette von Funktionsbausteinen in der IT-Infrastruktur darstellen und aufzeigen, welche Auswirkungen bestimmte Einflüsse haben. Das ist eine der wichtigsten Voraussetzungen in den Risikoabschätzungen. Nur so können wir im Fall der Fälle angemessen und schnell reagieren. Ich muss zudem genügend Redundanzen schaffen, um die Infrastruktur verlässlich betreiben zu können.“, weiß Dr. Kuhrau.

Dazu haben sein Team und er ein internes Konzept von Risikoklassen aufgestellt, das zentrale Systeme definiert, die immer redundant angelegt werden müssen. Darunter gibt es andere Risikoklassen von Prozessen oder unterstützenden Systemen, die sich in der Bedeutung für den Gesamtprozess der Einrichtung unterscheiden. All diese Strukturen werden mit dem ISMS kontrolliert und einem stetigen Review unterzogen.

Alles was bei der ATEGRIS in dieser Hinsicht entwickelt wird, prüft der Consulting-Partner gegen. „Die Umsetzung unseres Planes ist schließlich Neuland für uns, CETUS hat da bereits Erfahrung. Gerade bei der Formulierung von Leitlinien ist es sehr hilfreich, jemanden an der Seite zu haben, der sich auskennt. Das erspart uns viel Mühe und ist deutlich zielführender“, sagt Dr. Martin Kuhrau.

Erste Ergebnisse der harten Arbeit im vergangenen Jahr sind zu sehen. Zum Anschluss 2017 wurde ein Statusbericht erstellt, um die Geschäftsführung über den Fortgang der Projekte zu informieren. „Wir haben die 70 Prozent mittlerweile erreicht, sagt Tobias Puhe nicht ohne Stolz.

Kontakt:

CETUS Consulting GmbH
Mendelstraße 11

48149 Münster

0251- 980 1620

info@cetus-consulting.de

CETUS
Health · IT · Leadership